The IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Case No. 24 CR 503**
	)	
MARQUELL DAVIS,	)	
RAMONE BRADLEY, and	)	
EDMUND SINGLETON,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge:

Defendant Edmund Singleton has filed a motion to suppress evidence that was recovered as a result of law enforcement searching, pursuant to search warrants, three cell phones allegedly belonging to him. The Court understands that the government intends to offer at trial information obtained from the phones, including tracking data, phone numbers, text messages, and videos and pictures of Singleton. Singleton also contends that the government used information from the search of one or more of the phones to obtain separate search warrants that produced additional material that the government intends to offer at trial. Singleton asks the Court to suppress from evidence all the fruits obtained from the searches of the cell phones. He argues that the searches violated his Fourth Amendment rights because the 2022 warrant was facially invalid. For the reasons below, the Court denies the motion to suppress.

Background

Edmund Singleton, Marquell Davis, and Ramone Bradley were indicted on charges related to carjackings at two different Chicago gas stations on November 3, 2022. Surveillance footage shows one individual driving two others to each gas station, where the two passengers confronted with guns the drivers of two cars and attempted to forcibly steal the cars, in one case successfully. The government contends that Singleton was the person driving the vehicle that transported the two others.

Based on his alleged involvement in the carjackings, Singleton was charged with conspiracy to take a motor vehicle that had been transported or shipped in interstate commerce from the presence of another person by force and violence and by intimidation, with the intent to cause serious bodily harm, in violation of 18 U.S.C. § 371 (count one); violations of the federal carjacking statute, 18 U.S.C. § 2119 (counts two and four); a violation of 18 U.S.C. § 924(c)(1)(A) based on use of a firearm in relation to a crime of violence (count three); and a violation of 18 U.S.C. § 922(g) for unlawful possession of a firearm after conviction for a felony (count five).

Two cell phones were seized from Singleton at the time of his arrest: a purple iPhone in a silver case and a white iPhone in a black "Backwoods" case. A third cell phone was found in the backpack that Davis was carrying at the time of his arrest; it was a black iPhone in a "Supreme" case.

The Chicago Police Department detective assigned to the case, Adam Siegel, applied for warrants to search the three cell phones. The warrant applications (almost identical for each phone) explained the facts of the offense and the basis for conducting a search of the phones. A Cook County judge issued the warrants on December 6,

2022.

The warrants authorized law enforcement to search for eleven categories of material on the cell phones:

1) All records of incoming and outgoing phone calls;
2) All memory speed dial and redial features;
3) All voice mails;
4) All contact and address book information;
5) All incoming and outgoing messages and identification information for the senders and recipients including but not limited to text messages, SMS messages, social-networking messages or alerts;
6) All incoming and outgoing e-mails and e-mail addresses;
7) Proof of ownership of the cell phone including caller information.
8) All documents and files, including but not limited to: photos, video, audio, TXT, PDF, DOC, HTML files, APPS (applications);
9) All internet history or temporary files;
10) All deleted files or data.
11) All GPS location information

which have been used in the commission of, which constitute evidence of, or which constitute the fruits of the offenses of Armed Robbery 720 ILCS 5/18-2.

Def.'s Ex. 1.

The searches performed pursuant to these warrants resulted in the recovery of, among other things, photographs of Singleton's driver's license, usernames and passwords to an email account seemingly associated with Singleton, location information, and photos of firearms and of Singleton holding firearms. Singleton further contends that the 2022 search led law enforcement to his social media accounts, where it obtained information the government may use against him at trial.

Singleton also argues that evidence obtained from the 2022 warrants served as the basis for two additional search warrants that the government obtained in 2024. On August 7, 2024, Magistrate Judge Young B. Kim of this District issued search warrants directed at T-Mobile seeking cell site location information in connection with two cell

phone numbers allegedly used by Singleton. Def.'s Ex. 2. The warrants permitted the collection of data including names, addresses, local and long-distance telephone connection records and session times, and records relating to wire and electronic communications. *Id*. The affidavits submitted to obtain these warrants referred to data obtained from the 2022 search, as well as factual allegations that had been included in the 2022 search warrant applications. The location information obtained from the search pursuant to the 2024 warrants revealed that one of the phones emitted signals to cell towers that allegedly corresponded to the location of the carjacking offenses.

Singleton maintains that the probable cause supporting the 2024 warrants depended entirely on evidence obtained via the allegedly overbroad 2022 warrants and that, as a result, evidence from the latter searches should be suppressed as well.

Discussion

As the Court has indicated, Singleton argues that the Court should suppress evidence obtained via the 2022 and 2024 search warrants because the 2022 warrants were overly broad and not particularized.

As the Supreme Court has noted, data from a cell phone allows one to reconstruct "the sum of an individual's private life." *Riley v. California*, 573 U.S. 373, 394 (2014). "American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." *Id.* at 395 (internal citation omitted). It is precisely this breadth and depth of the data that can be stored on an individual's phone that demands heightened attention towards the scope of a warrant

issued to search such a phone. *See id.* at 403 (explaining that modern cell phones contain the "privacies of life" for Americans and must be granted the same protections the founders fought for in the Fourth Amendment); *Socha v. City of Joliet*, 107 F.4th 700, 709 (7th Cir. 2024). Accordingly, the Seventh Circuit has cautioned that a warrant's "[p]articularity is of substantial importance in the context of cell phones." *Socha*, 107 F.4th at 709.

The Fourth Amendment requires a warrant to "describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging through one's belongings." *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010). As the Court has noted, this requirement is particularly important when dealing with a cell phone, given the nature and amount of information that can be stored there. Thus, law enforcement has an "obligation to be specific and explain why there is probable cause to search every part of a cell phone they seek to search." *Socha*, 107 F.4th at 709–10.

That said, specificity is "relative," and a warrant "need not be more specific than knowledge allows." *United States v. Bishop*, 910 F.3d 335, 338 (7th Cir. 2018). In other words, law enforcement is required to particularize a warrant only to the extent it is reasonably able to do so based on the facts it knows at the time it obtains the warrant. *See id.* Officers' knowledge about the evidence they are looking for and where it may be found on a cell phone is thus significant in determining whether a warrant is sufficiently particularized. *See id.*; *see also Socha*, 107 F.4th at 709–10.

The government argues that this case is similar to *Bishop*. In *Bishop,* the Seventh Circuit found that a warrant that authorized the search of all data files on an individual's phone related to a particular type of crime was sufficiently particularized.

See Bishop, 910 F.3d at 338. The warrant defined the things to be seized as "any evidence (including all photos, videos, and/or any other digital files, including removable memory cards) of suspect identity, motive, scheme/plan along with DNA evidence of the crime of Criminal Recklessness with a deadly weapon which is hidden or secreted [in the cellphone or] related to the offense of Dealing illegal drugs." *Id.* The Seventh Circuit concluded that this seemingly broad warrant was facially valid because of two reasons: it "cabin[ed] the things being looked for by stating what crime is under investigation" and "the police did not know where on his phone Bishop kept his drug ledgers and gun videos . . . . This warrant was as specific as circumstances allowed." *Id.* at 337-38.

The government argues, that in this case, "[l]ike in Bishop, the police here 'did not know where on his phone' Singleton kept evidence of his carjackings – in text messages, on messaging apps, in photos, on his phone's GPS data, etc." Gov't's Resp. Br. at 14 (citing *Bishop*, 910 F.3d at 338). The government further argues that:

> more detailed particularity about evidentiary items on the phone was impossible. The state search warrants were as particular as the circumstances reasonably permitted. The police did not know where on the phone the evidence would be located or the form that evidence would take. . . . Even as to date ranges, limiting the state warrants for the cell phones to the date immediately before and after the offenses is not required where, as here, officers did not know the extent of the planning and preparation for these offenses.

Gov't's Resp. Br. at 13.

The Court has a hard time seeing how it was, as the government contends, "impossible" to make the warrants in this case more particularized. Specifically, it is hard to see why the warrants could not and should not have been date-limited regarding the files they allowed law enforcement to search. The warrants, as they stood,

essentially allowed the search of every file on each phone, without regard to its creation date—even files created years before the carjackings. Even considering, as the government argues, that the officers did not know how long the suspects had been planning the crime, there was still some reasonable date range they could have used. Similarly, even if law enforcement did not know which applications held relevant evidence, it did know of the other suspects and thus could have limited searches of and seizures from these applications and files to only those revealing communications between Singleton and the other suspects, or perhaps that along with communications on the dates immediately surrounding the carjackings.

Bishop does not call for a different result. Though it is true, as the government contends, that under *Bishop* a warrant should "cabin[] the things being looked for by stating what crime is under investigation"—as the warrants at issue here did—the analysis does not end there. *See Bishop*, 910 F.3d at 337. The Seventh Circuit went on to state that "if some more-specific alternative would have done better at protecting privacy while still permitting legitimate investigation," "[a] warrant may be thought 'too general.'" *Id.* That would appear to be the case here. Unlike in *Bishop*, in which at least one of the offenses (drug dealing) likely occurred over a period of time, here the government was investigating two discrete crimes that took place on a single date.

Socha likewise does not call for a different result. In *Socha*, the Seventh Circuit suggested that a broad warrant might be valid in a case in which law enforcement had no knowledge of what sort of evidence it was looking for on a phone. *See Socha*, 107 F.4th at 710 ("This broad language would be proper if not for the fact that officers knew exactly what evidence they were looking for and, as a matter of common knowledge,

where it might be found: a single text message in her text history."). But just as this principle was not applicable in *Socha*—because officers *did* know what evidence they were looking for—it does not apply here. As the Court has noted, based on what law enforcement knew, it would have been relatively simple to provide a date and/or a date-plus-subject limitation.

For these reasons, the Court concludes that the 2022 warrant was not sufficiently particularized.

B. Good faith exception

The government argues that even if the 2022 warrants were not sufficiently particularized, evidence obtained as a result should not be excluded, because Detective Siegel relied in good faith on the state court judge's decision to issue the warrants. *See United States v. Leon*, 468 U.S. 897, 922 (1984); *United States v. Rees*, 957 F.3d 761, 771 (7th Cir. 2020) ("Even if the search warrants lacked a basis in probable cause, the exclusionary rule does not operate against the evidence if the good-faith exception applies—that is, if the officers who executed the warrants relied, in objective good faith, on the magistrate's probable-cause decision.").

Detective Siegel's choice to seek a warrant in the first place "invokes a presumption that he acted in good faith." *Rees*, 957 F.3d at 771 Additional factors supporting a finding of good faith are the fact that he "conferr[ed] with a prosecutor before applying for a warrant," and that he "rel[ied] on the judge's issuance of the warrant." *Socha,* 107 F.4th at 710. Indeed, "an officer cannot ordinarily be expected to question a judge's probable cause determination." *United States v. Lickers*, 928 F.3d 609, 619 (7th Cir. 2019).

The inquiry does not end there, however. The Court next asks whether Singleton has offered evidence that overcomes the presumption of good faith. There are four well-established situations in which a defendant may overcome this presumption:

> (1) the affiant misled the magistrate with information the affiant knew was false or would have known was false but for the affiant's reckless disregard for the truth; (2) the magistrate wholly abandoned the judicial role and instead acted as an adjunct law-enforcement officer; (3) the affidavit was bare boned, 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'; and (4) the warrant was so facially deficient in particularizing its scope that the officers could not reasonably presume it was valid.

Rees, 957 F.3d at 771 (internal citations omitted). Singleton says this case presents the third situation, where "the warrant was so facially deficient in particularizing its scope that the officers could not reasonably presume it was valid." *Id.* In assessing this, the analysis is "confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n. 23; *see also United States v. Dickerson*, 975 F.2d 1245, 1250 (7th Cir. 1992); *Taylor v. Hughes*, 26 F.4th 419, 429–30 (7th Cir. 2022).

Singleton points to *United States v. Glover*, 755 F.3d 811 (7th Cir. 2014), to support a contention that the good faith exception does not apply *at all* when a warrant is insufficiently particularized. *See id.* at 814. But although the court in *Glover*, quoting *Leon*, said that the good faith exception does not apply "when the warrant is facially deficient in that it fails to specify the place to search or the items to seize," *id.* at 819 (quoting *Leon*, 468 U.S. at 923), *Glover* itself did not involve a warrant claimed to be invalid due to insufficient particularization. Rather, the issue in that case was the claimed insufficiency of the affidavit supporting the issuance of the warrant. And the

court concluded that even though the warrant lacked a sufficient probable cause basis, the good faith exception applied with respect to the contention that the supporting affidavit was patently deficient, because "the affidavit was not . . . lacking in factual detail to the point that reliance was unreasonable." *Id.* In short, *Glover* does not help Singleton here.[1] And he has cited no case that finds a warrant to be so "bare bones" that the good faith exception was found not to apply.

Turning to *Leon* itself—the source of the rule quoted in *Glover*—the full sentence quoted reads: "Finally, depending on the circumstances of the particular case, a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923. This quite plainly does not mean that the good faith exception does not apply when a violation of the particularization requirement is *claimed*. Rather, it indicates that in particular circumstances, police executing a warrant that "fail[s] to particularize the place to be searched or the things to be seized" might be unable to invoke the exception.

In the Court's view, *Socha* makes it clear that the good faith exception applies in this case despite Singleton's claim that the warrant was insufficiently particularized. In *Socha*—a civil suit under 42 U.S.C. § 1983—the Seventh Circuit suggested that the warrant at issue was insufficiently particularized because it permitted the officer to search for:

> [a]ny and all data regarding electronic communications, including dates and times of those communications, digital images or videos, e-mail, voice mail, buddy lists,

[1] The court in *Glover* separately remanded the case for a hearing on good faith with respect to certain alleged omissions from the warrant application, but that does not impact the issues in the present case.

> chat logs, instant messaging or text accounts, forensic data as well as data pertaining to ownership and registration of the device, any and all access logs identifying who utilized said digital storage devices, and any "hidden," erased, compressed, password-protected, or encrypted files.

Socha, 107 F.4th at 706. Specifically, the court stated that the warrant's "broad language *would be proper if not for the fact* that officers knew exactly what evidence they were looking for and, as a matter of common knowledge, where it might be found: a single text message in her text history." *Id.* at 710 (emphasis added). But despite indicating that the warrant was too broad, the Court still found that the officer was entitled to qualified immunity, applying a standard essentially indistinguishable from the objective good faith standard under *Leon*. *See id*. Specifically, the Court cited *Messerschmidt v. Millender*, 565 U.S. 535 (2012), which states that the application of qualified immunity "generally turns on the objective legal reasonableness of the action, assessed in light of the legal rules that were clearly established at the time it was taken." *Id.* at 546 (internal quotation marks omitted). This is the same as the standard under *Leon*, as the Supreme Court recognized in *Messerschmidt. See id.* at 546 (citing *Leon*, 468 U.S. at 922-23) & n.1 ("[T]he same standard of objective reasonableness that we applied in the context of a suppression hearing in *Leon* defines the qualified immunity accorded an officer . . . ." (quoting *Malley v. Briggs*, 475 U.S. 335, 344 (1986)).

The warrant in *Socha* was insufficiently particularized because it effectively authorized a search and seizure of any file on the party's cell phone even though law enforcement was looking for a single text message. And yet the Seventh Circuit ruled that the officer's reliance on the overly broad warrant was objectively reasonable. Given that holding, it is clear that the good faith exception applies in the present case as well—particularly because the nature and quantum of evidence on the cell phones

relating to the carjackings was legitimately understood as potentially far broader than the single text message that was being sought in *Socha*.

For these reasons, the Court concludes that the good faith exception applies to the 2022 search warrants. As a result, evidence derived from the 2022 warrants is admissible. And for that reason, Singleton's challenge to the 2024 search warrants likewise fails. The Court therefore denies Singleton's motion to suppress.

Conclusion

For the foregoing reasons, the Court denies the defendant's motion to suppress [dkt. no. 65].

Date: June 18, 2025

MATTHEW F. KENNELLY
United States District Judge